

ケーブル技術スタッフの機器チェック!

日々開発されるケーブルテレビ関連機器を、技術スタッフが厳しい目でチェック! 実用性に焦点を当てて報告します。

No. 58

3ウェイハンドシェイク

豊島ケーブルネットワーク(株) 技術部 部長 上山裕史

今回はWindows XPのサポート終了に関連した話題について紹介します。

私たちケーブルテレビ局の技術者は、ISP(インターネット・サービス・プロバイダ)として、顧客のセキュリティや自ネットワークからの不正パケットの送出を防ぐために、不断の努力をしています。今回はWindows XP(以下、XP)のサポート終了に伴い、ひょっとすると遭遇するかもしれない障害を紹介いたします。

XPは2014年4月にサポートを終了すると、マイクロソフトからアナウンスされています。XP後継のVISTA以降TCP/IPプロトコルの3ウェイハンドシェイクに、RFC 1323で定めるウィンドウスケールリングのオプションの追加がありました。DOCSIS3.0の導入が始まり、高速通信のため自動でバッファサイズのネゴシエーションを行います。

会社組織のインターネット接続は、ファイヤーウォールが持つNAT(Network Address Translation:アドレス変換機能)を利用する場合があります。社内をプライベートIPアドレスで統一し、図1に示すように外部に接続する時だけNATでグローバルIPアドレスに変換する仕組み

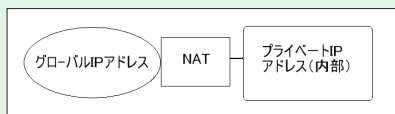


図1:NATの利用

です。古いバージョンのファイヤーウォールでは、VISTA以降サポートされたオプションをチェックサムエラーのある不正パケットとみなし破棄する場合がありますので、XPだけで構築されたネットワークを更新する場合、ファイヤーウォールのバージョンアップも必要になります。

図2は3ウェイハンドシェイクの様子を示します。3ウェイハンドシェイクでは、①syn送出で通信したいWWWサーバに向けてSYNパケットを送出します。SYNパケットを受け取ったWWWサーバは、ウィンドウスケールリングのオプションが使用可能なことを②syn/ack送出で伝えます。これを理解したPCクライアントは、③ack送出を行います。これが正常なシーケンスですが、古いバージョンのファイヤーウォールでは、②

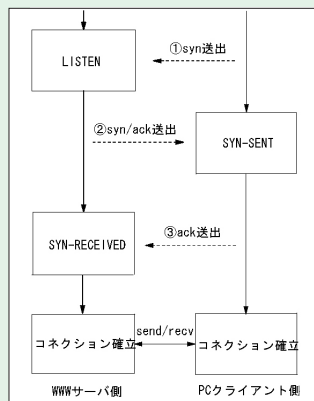


図2:3ウェイハンドシェイク

syn/ackパケットをチェックサムエラーのある不正なパケットとして破棄します。これを本誌2012年9月号で紹介したフリーソフトワイヤシャークでキャプチャ・解析した様子を図3に示します。

図3はウィンドウスケールリングのオプションで拡張されたため、12バイトのオプションエリアがあることがわかります。

図4は、XPのパケットでオプションが8バイトのエリアであることがわかります。結果的に③ack送出が無いので、WWWサーバ側では最低でも30秒間データを保持することになります。これはSYN flood攻撃と同じ手法になってしまうので、WWWサーバ管理者を神経質にさせることになります。ケーブルテレビ局の技術者は、メールサーバやWWWサーバのアウトソーシング化でインターネットの知識が不要になることはありません。顧客へのサービス品質を上げるために自ネットワークのクリーン化を進めると同時に、ワイヤシャークのようなパケット解析を駆使して現象を解明し、障害を解決していかなければならないと考えます。

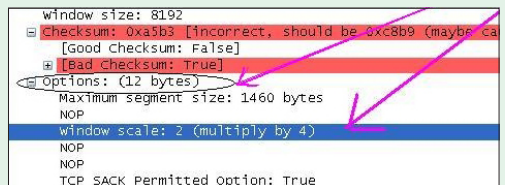


図3:オプション有り

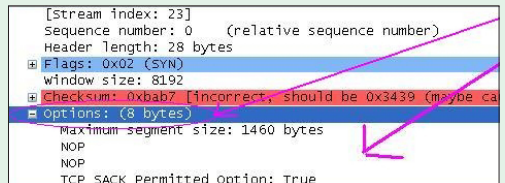


図4:オプション無し